SPYWOLF

Security Audit Report

Completed on

February 24, 2023

OVERVIEW

This audit has been prepared for **JAGUAR** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

JAGUAR

PROJECT DESCRIPTION

According to their whitepaper:

Jaguar offer passive income solutions in the crypto market with a complete ecosystem of tools for holders and project partners. With their Staking platform, holders can earn passive income.

Release Date: Presale starts in February, 2023

Category: Staking

CONTRACT INFO

Token Name	Symbol
Jaguar	JGR

Contract Address
0x0bEC38a2f00eF873f35Cd8E75a25Ffe716df7dd2

Network	Language
Binance Smart Chain	Solidity

Deployment Date	Verified?
Feb 23, 2023	Yes

Total Supply	Status
100,000	Not Launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	4
Uniq Senders	1
Uniq Receivers	4
Total Amount	99999.99999999999 JGR
Median Transfer Amount	30000 JGR
Average Transfer Amount	24999.999999999996 JGR
First transfer date	2023-02-23
Last transfer date	2023-02-23
Days token transferred	1

SMART CONTRACT STATS

Calls Count	6
External calls	6
Internal calls	0
Transactions count	6
Uniq Callers	1
Days contract called	1
Last transaction time	2023-02-23 18:02:32 UTC
Created	2023-02-23 17:49:35 UTC
Create TX	0x292a441eccea5d677e8b859a82ce098807cbe8028cd500891f84b3c7d680a36c
Creator	0x7b77bcb5068c28a52aa3c674ebca4ca2ba1bbc07

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Manual and autoBuyBack fails, leading to inability to sell if autobuyback is enabled.

```
function triggerManualBuyback(uint256 amount, bool triggerBuybackMultiplier) external authorized {
    buyTokens(amount, DEAD);
    if(triggerBuybackMultiplier){
        buybackMultiplierTriggeredAt = block.timestamp;
        emit BuybackMultiplierActive(buybackMultiplierLength);
    }
}

function triggerAutoBuyback() internal {
    buyTokens(autoBuybackAmount, DEAD);
    autoBuybackBlockLast = block.number;
    autoBuybackAccumulator = autoBuybackAccumulator.add(autoBuybackAmount);
    if(autoBuybackAccumulator > autoBuybackCap){ autoBuybackEnabled = false; }
}

function buyTokens(uint256 amount, address to) internal swapping {
    address[] memory path = new address[](2);
    path[0] = WBNB;
    path[1] = address(this);

    router.swapExactETHForTokensSupportingFeeOnTransferTokens{value: amount}(
        0,
        path,
        to,
        block.timestamp
    );
}
```

- Recommendation:
  - Consider adding approval for router tokens spending, review tokens swap path.

FOUND THREATS

⚠ High Risk

Owner can change token's auto buyback criteria.
If autoBuybackEnabled variable is true, autoBuybackAmount variableis 0 and contract's token balance is 0, buyback will fail and cause all sells to fail.

```
function setAutoBuybackSettings(bool _enabled, uint256 _cap,
uint256 _amount, uint256 _period) external authorized {
    autoBuybackEnabled = _enabled;
    autoBuybackCap = _cap;
    autoBuybackAccumulator = 0;
    autoBuybackAmount = _amount;
    autoBuybackBlockPeriod = _period;
    autoBuybackBlockLast = block.number;
}

function _transferFrom(address sender, address recipient,
uint256 amount) internal returns (bool) {
.............
if(shouldAutoBuyback()){ triggerAutoBuyback(); }
.............
}

function shouldAutoBuyback() internal view returns (bool) {
.................
&& autoBuybackEnabled
&& address(this).balance >= autoBuybackAmount;
.................
}

function triggerAutoBuyback() internal {
buyTokens(autoBuybackAmount, DEAD);
..........
}

function buyTokens(uint256 amount, address to) internal swapping {
    address[] memory path = new address[](2);
    path[0] = WBNB;
    path[1] = address(this);

    router.swapExactETHForTokensSupportingFeeOnTransferTokens
    {value: amount}(
        0,
        path,
        to,
        block.timestamp
    );
}
```

- Recommendation:
  - Consider adding approval for router tokens spending, review tokens swap path, ensure that autoBuyBackAmount is always above 1 token and take decimals into consideration.

FOUND THREATS

⚠ High Risk

Owner can enable/disable token transfers.

When token transfers is disabled, any transfers from unauthorized addresses will be forbidden. This includes buys/sells and transfers.

```
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
..............
if(!authorizations[sender] && !authorizations[recipient]){
        require(emergBlock,"Trading not open yet");
}
..............
}

function EmergencyTradeBlock() public authorized {
    emergBlock = false;
}

function TradeUnblock() public authorized {
    emergBlock = true;
}
```

- Recommendation:
  - Once enabled trade should not be disabled again.

FOUND THREATS

⚠ High Risk

Owner can set max transaction limits for buys and sells without limitations.
If max transaction limit is set to low number, this can lead to inability to buy/sell.
When transaction limitations are applied, users will be subject to transfer restrictions to certain amounts (depending ot current setting).

```
function setTxLimit(uint256 BuyAmount, uint256 SellAmount) external authorized {
    _maxTxBuyAmount = BuyAmount;
    _maxTxSellAmount = SellAmount;
}
```

- Recommendation:
  - Considered as good transaction limitation practice is transaction amount to be equal or higher than 0.1% of total supply.

FOUND THREATS

⚠ High Risk

Owner can change auto swap settings.
AutoSwap mechanism is failing.
If auto swap is set to 0 and contract's balance is equal to 0, selling will fail.

```
function setSwapBackSettings(bool _enabled, uint256 _amount) external authorized {
    swapEnabled = _enabled;
    swapThreshold = _amount;
}
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
.............
if(shouldSwapBack()){ swapBack(recipient == pair); }
.............
}

function shouldSwapBack() internal view returns (bool) {
.............
&& swapEnabled
&& _balances[address(this)] >= swapThreshold;
.............
}

function swapBack(bool selling) internal swapping {
.............
uint256 amountToLiquify = balanceOf(address(this)).mul(dynamicLiquidityFee).div(totalFee).div(2);
uint256 amountToSwap = balanceOf(address(this)).sub(amountToLiquify);

address[] memory path = new address[](2);
path[0] = address(this);
path[1] = WBNB;
uint256 balanceBefore = address(this).balance;

router.swapExactTokensForETHSupportingFeeOnTransferTokens(
    amountToSwap,
    0,
    path,
    address(this),
    block.timestamp
);
.............
}
```

- Recommendation:
  - Consider adding approval for router tokens spending, review tokens swap path, ensure that swapThrehold is always above 1 token.

FOUND THREATS

⚠ Medium Risk

Owner can set buy/sell fees up to 25%.
Combined buy+sell=50%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
uint256 maxfee = 2500;

function setBuyFees(uint256 _liquidityFee, uint256 _marketingFee,
uint256 _projectFee,  uint256 _buyfeeburning) external authorized {
    liquidityBuyFee = _liquidityFee;
    marketingBuyFee = _marketingFee;
    projectBuyFee = _projectFee;
    buyfeeburning = _buyfeeburning;
    totalBuyFee = _liquidityFee.add(_marketingFee).add(_projectFee).add(_buyfeeburning);
    require(totalBuyFee < maxfee);
    require(totalBuyFee < buyFeeDenominator);
}

function setSellFees(uint256 _liquidityFee, uint256 _marketingFee,
uint256 _projectFee, uint256 _sellfeeburning) external authorized {
    liquiditySellFee = _liquidityFee;
    marketingSellFee = _marketingFee;
    projectSellFee = _projectFee;
    sellfeeburning = _sellfeeburning;
    totalSellFee = _liquidityFee.add(_marketingFee).add(_projectFee).add(_sellfeeburning);
    require(totalSellFee < maxfee);
    require(totalSellFee < sellFeeDenominator);
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 50%.

FOUND THREATS

⚠ Medium Risk

Owner can change fee receiver addresses.
If address that is not able to receive BNB is selected, swapBack() function will fail causing all further sells to fail.

```
function setFeeReceivers(address _autoLiquidityReceiver, address _marketingFeeReceiver,
address _projectFeeReceiver) external authorized {
    autoLiquidityReceiver = _autoLiquidityReceiver;
    marketingFeeReceiver = _marketingFeeReceiver;
    projectFeeReceiver = _projectFeeReceiver;
}

function swapBack(bool selling) internal swapping {
..............
if (marketingFee > 0) {
uint256 amountBNBMarketing = amountBNB.mul(marketingFee).div(totalBNBFee);
(bool success, /* bytes memory data */) = payable(marketingFeeReceiver).call
{value: amountBNBMarketing, gas: 50000}("");
require(success, "receiver rejected ETH transfer");
}

if (projectFee > 0) {
uint256 amountBNBproject = amountBNB.mul(projectFee).div(totalBNBFee);

(bool success2, /* bytes memory data */) = payable(projectFeeReceiver).call
{value: amountBNBproject, gas: 30000}("");
require(success2, "receiver rejected ETH transfer");}
..............
}
```

FOUND THREATS

⚠ Medium Risk

Initiate launch() manually to avoid unwanted behaviour as launch() have authorized modifier.

```
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
...........
if(!launched() && recipient == pair) {
    require(_balances[sender] > 0);
    launch();
}
...........
}

function launched() internal view returns (bool) {
    return launchedAt != 0;
}

function launch() public authorized {
    require(launchedAt == 0, "Already launched");
    launchedAt = block.number;
    launchedAtTimestamp = block.timestamp;
}
```

FOUND THREATS

⚠ Low Risk

Owner can change multiplier settings.
Sell fees might be up to 50% in the first 24 hours after token's launch.

```
function setBuybackMultiplierSettings(uint256 numerator,
uint256 denominator, uint256 length) external authorized {
    require(numerator / denominator <= 2 && numerator > denominator);
    buybackMultiplierNumerator = numerator;
    buybackMultiplierDenominator = denominator;
    buybackMultiplierLength = length;
}


function getTotalFee(bool selling) public view returns (uint256) {
    .........
    if(selling){ return getMultipliedFee(); }
   .......
}

function getMultipliedFee() public view returns (uint256) {
    if (launchedAtTimestamp + 1 days > block.timestamp) {
        return totalSellFee.mul(10000).div(sellFeeDenominator);
    }

    else if (buybackMultiplierTriggeredAt.add(buybackMultiplierLength) > block.timestamp) {
        uint256 remainingTime = buybackMultiplierTriggeredAt.add(buybackMultiplierLength).sub(block.timestamp);
        uint256 feeIncrease = totalSellFee.mul(buybackMultiplierNumerator).div(buybackMultiplierDenominator).sub(totalSellFee);
        return totalSellFee.add(feeIncrease.mul(remainingTime).div(buybackMultiplierLength));
    }

    return totalSellFee;
}
```

Informational

Owner can exclude address from dividends.
Addresses excluded from dividends wont receive reward token as dividend.

```
function setIsDividendExempt(address holder, bool exempt) external authorized {
    require(holder != address(this) && holder != pair);
    isDividendExempt[holder] = exempt;
    if(exempt){
        distributor.setShare(holder, 0);
    }else{
        distributor.setShare(holder, _balances[holder]);
    }
}
```

Owner can withdraw any tokens from the contract.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function savetokens(address account, uint256 _quant,
address _tokenrec) external onlyOwner() {
  quantrec = _quant;
  tokenrec = _tokenrec;
  IBEP20(tokenrec).transfer(account, quantrec);
}

function manualSend() external authorized {
    uint256 contractETHBalance = address(this).balance;
    uint256 realamount = (contractETHBalance);
    payable(marketingFeeReceiver).transfer(realamount);
}
```

Informational

Owner can set cooldown period between trades up to 255 seconds.

When applied, users should wait the period set to make more than 1 buy.
Current cooldown period is 30 seconds.

```
function cooldownEnabled(bool _status, uint8 _interval) public onlyOwner {
    buyCooldownEnabled = _status;
    cooldownTimerInterval = _interval;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

JAGUAR

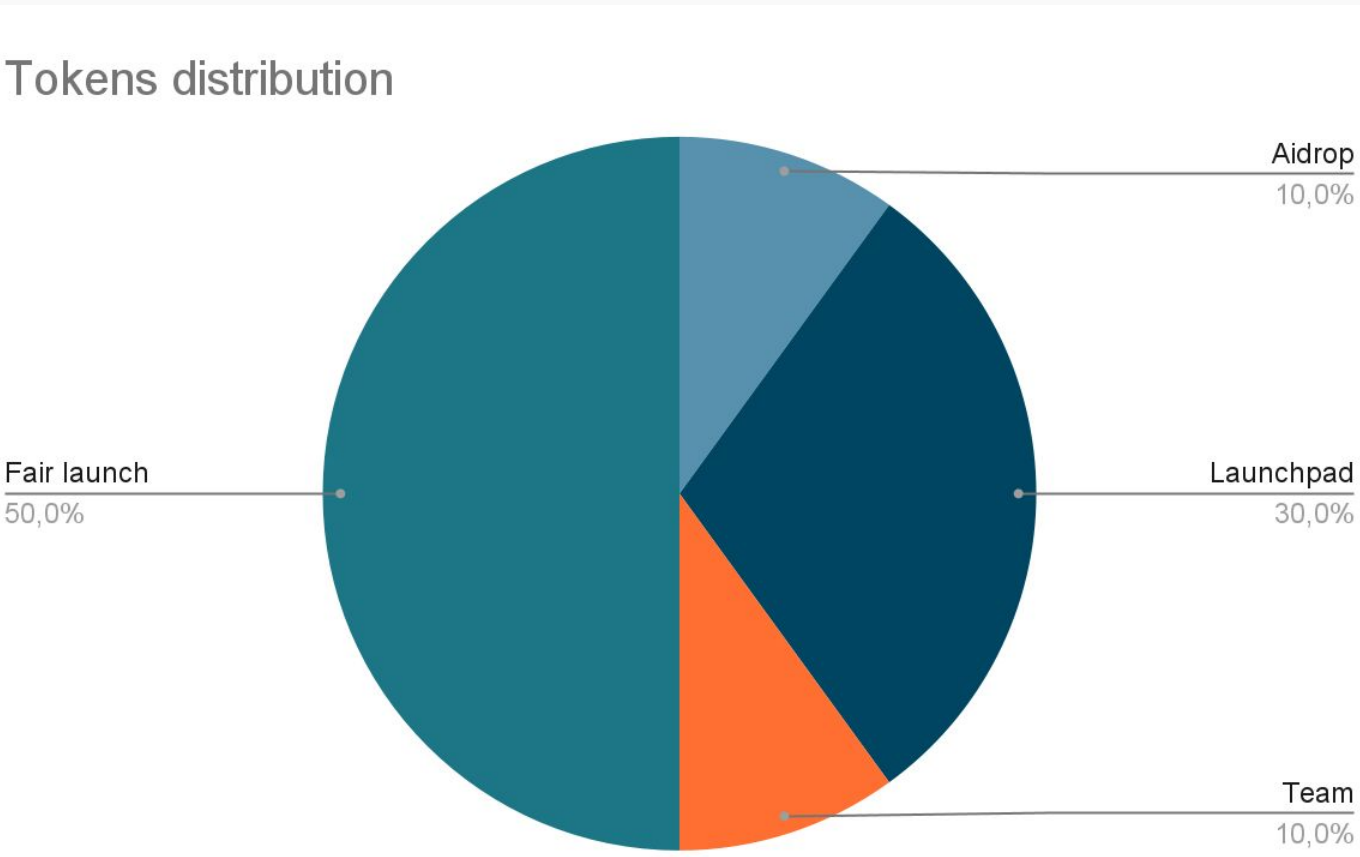
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 30% - Launchpad
- 10% - Airdrop
- 10% - Team
- 50% - Fair Launch



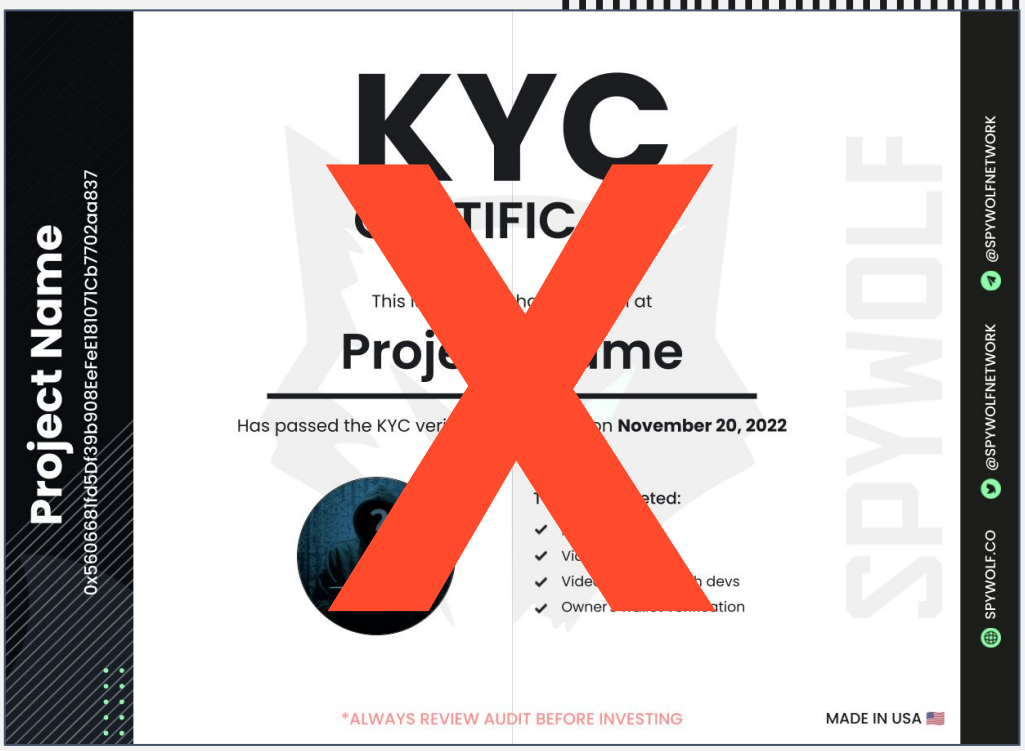
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://cryptojaguar.co

Domain Registry
publicdomainregistry.com

Domain Expiration
Expires on 2024-02-19

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design, appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. Few grammar mistakes found.

Whitepaper
Yes, explanatory.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes

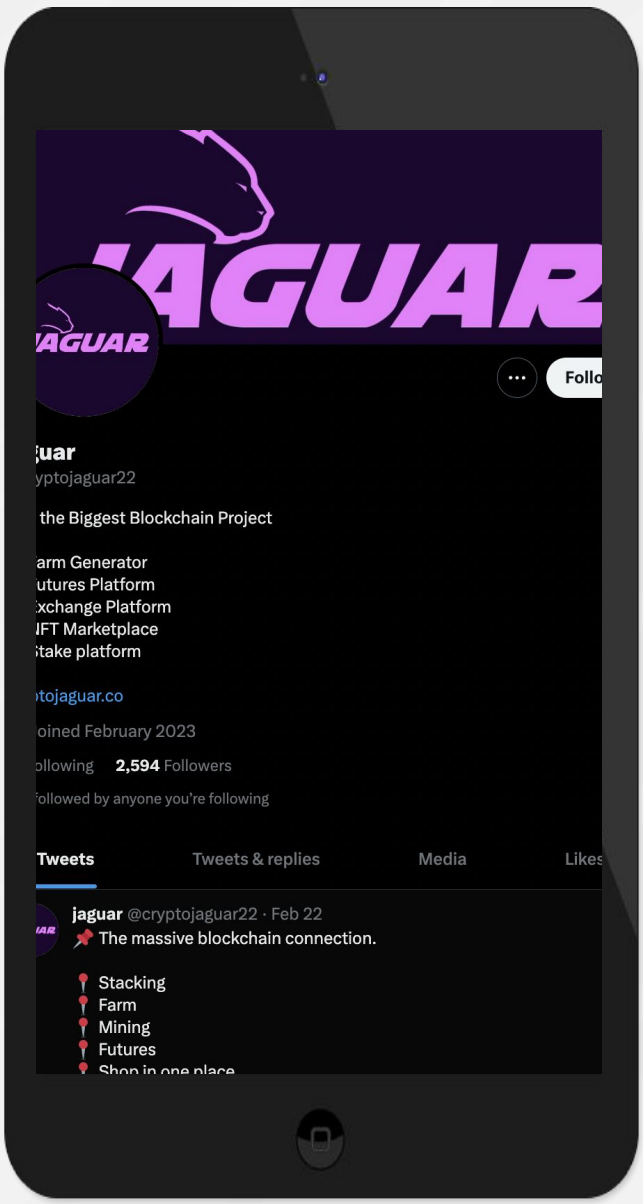
cryptojaguar.co

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active.



Twitter

@cryptojaguar22

- 2 594 followers
- Active
- 5 total posts

Discord

- Not available

Telegram

@jaguarcommunityofficial

- 2 890 members
- Few active members.
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 400 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.